


KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	SECTION NUMBER 05-161	PAGE NUMBER
		SUBJECT: INFORMATION TECHNOLOGY AND RECORDS: Data Management and Administration	

The IMPP has been placed on RESERVE status, reason being is that the viable content of this IMPP has been subsumed within the parameters of IMPP (05-163) being issued at this time.

Secretary of Corrections

06-02-04
Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-161

**Title: INFORMATION TECHNOLOGY AND RECORDS: Data
 Management and Administration**

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 09-21-02, was reviewed during January 2004 by the KDOC Policy Review Panel, per IMPP 01-101. At the time of this annual review, the Policy Review Panel determined that: no substantive changes and/or modifications to this IMPP are necessary at this time, and the IMPP shall remain in effect as issued on the above stated date.

The next scheduled review for this IMPP is January 2005.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.

Norman Bacon, IT Acting Director
Policy Review Committee Chairperson

Date

Roger Werholtz, Secretary of Corrections

02-03-04
Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-161

**Title: INFORMATION TECHNOLOGY AND RECORDS: Data
 Management and Administration**

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 09-21-02, was reviewed during January 2003 by the KDOC Policy Review Panel, per IMPP 01-101. At the time of this annual review, the Policy Review Panel determined that: no substantive changes and/or modifications to this IMPP are necessary at this time, and the IMPP shall remain in effect as issued on the above stated date.

The next scheduled review for this IMPP is January 2004.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.


Carlos Usera, Information Resource Manager
Policy Review Committee Chairperson

Date

Roger Werholtz, Secretary of Corrections

01-31-03
Date

KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	SECTION NUMBER 05-161	PAGE NUMBER 1 of 4
		SUBJECT: INFORMATION TECHNOLOGY AND RECORDS: Data Management and Administration	
Approved By: Secretary of Corrections		Original Date Issued:	N/A
		Current Amendment Effective:	09-21-02
		Replaces Amendment Issued:	N/A

POLICY

The Department of Corrections shall provide data management services to all organizations requiring access to digital information. Each staff member is responsible to protect critical data from loss or corruption to ensure continuity of core business activities.

Data shall be safeguarded utilizing any stable storage methods to include redundant storage arrays, parity checking devices, tape drives, optical storage, and storage management systems. Critical information must be backed up to removable medium, cataloged and stored in a Department approved secured site.

Information Technology Managers responsible for the management of data in the Department shall follow the below steps to ensure data availability:

- Determination of availability requirements
- Development of an availability plan
- Maintenance of redundant data sources
- Management of long-term data retention
- Monitoring and reporting on availability.

DEFINITIONS

Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned.

Data Administration: An ongoing, centralized, administrative function that coordinates the design, implementation, and maintenance of an effective data structure of the entities and relationships that comprise the integrated enterprise-wide database(s), and makes this information available to a community of information resource users. Responsibilities typically assigned to this function include information strategy planning, data and process modeling (both conceptual and logical), and the development of standards, policies, and procedures to define, collect, and organize data to meet managers' and users' existing and future information needs.

Data Custodian: Guardian or caretaker; the holder of data; the agent charged with the data owner's requirement for processing, communications, protection controls, access controls, and output distribution for the resource. The data custodian is normally a provider of services. The data custodian may be a central data center providing services to a number of agencies which are data owners.

Data Owner: The business function manager or agent assigned stewardship responsibility for the data resource.

Information: Data that have been organized or prepared in a form that is suitable for decision-making.

Policy

I. Data Management Policies

- A. Each facility and office shall have disaster recovery / contingency plan for mission-critical data.
- B. Each facility and office that houses servers shall utilize Department approved backup and recovery technology.
- C. Data management architectures shall be based on commonly accepted standards that are extensible, interoperable and scalable.
- D. All persons with access to data shall take actions to ensure the confidentiality of the records.
- E. Complete asset inventories must be maintained to assist in the back-up, recovery, and accessibility of the data used by these assets.
- F. Redundant hot sites shall be identified for long-term continuity purposes.

II. Responsibilities

- A. Director, Information Technology:
 - 1. Submit an annual report on the Data Administration Policy as defined in ITEC policy 8000

2. Notify the Kansas Information Technology Office on any changes to the status of the Agency Data Administrator.

B. Manager, Computer Operations:

1. Ensure that Department wide data is maintained in a manner that provides high availability, performance, and reliability to the staff.
2. Create and update daily reports that provide information on data back-ups, storage location, availability, retention and expiration schedules.
3. Implement centralized backup of critical file servers located throughout the state.

C. Records Custodian:

1. Serve as the Agency Data Administrator as defined in ITEC Policy 8000.
2. Determine and enforce records retention policy for electronic media.
3. Provide for the long-term storage of archived electronic and optical disk media.
4. Develop and implement strategies for data preservation that consider the projected life of the physical storage media, and the hardware and software used to store the data.
 - a. Strategy should provide for the refresh of physical media.
 - b. Shall consider the conversion of data to new formats or systems as necessary.
 - c. Define and assign data administration responsibilities to data owners and data custodians.

D. Network Administrators:

1. Ensure that locally used data is maintained in a manner that provides high availability, performance, and reliability to the staff.
2. Coordinate with facility and office staffs to determine appropriate back-up/recovery procedures.
3. Implement automated backup techniques and maintain back-up logs.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities who are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to either employees, offenders, or third parties. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

Daily Backup Logs

REFERENCES

Government Records Preservation Act (KSA 45-401 – KSA 45-413)

Open Records Act (KSA 45-215 – 45-223)

Public Records Act (KSA 75-3501 – KSA 75-3518)

Records made on Electronically-accessed Media; Authorization, Conditions and Procedures, Application, Notice to State Records Board (KSA 45-501)

Tampering with a Public Record (KSA 21-3821)

Freedom of Information Act (FOIA) – (5 USC 552) and Electronic Freedom of Information Act (E-FOIA) – (amendment to 5 USC 552)

General Records Retention and Disposition Schedule for State Agencies (KAR 53-3-1)

Records Officer (KAR 53-4-1)

Business Contingency Planning (ITEC Policy 3200)

Business Contingency Planning Implementation (ITEC Policy 3210)

Development of a Data Administration Program (ITEC Policy 8000)

Kansas State-wide Technical Architecture, Chapter 18

Kansas Electronic Records Management Guidelines,
<http://www.kshs.org/archives/ermguide.htm>.

ATTACHMENTS

None